FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0015

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: _____

Dated: 13 April 2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 3 april 2012

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1676	03/09/2012	Symantec Java Cryptographic Module Version 1.1	Symantec Corporation	Software Version: 1.1
1685	03/09/2012	ZyFLEX Crypto Module ZCM-100	ZyFLEX Technologies Incorporation	Hardware Version: AAM; Firmware Version: 1.1
1686	03/09/2012	McAfee Endpoint Encryption Client Windows Cryptographic Module 1.0 [1] and McAfee Endpoint Encryption Client Preboot Cryptographic Module 1.0 [2]	McAfee, Inc.	Software Version: 6.1.3
1687	03/30/2012	Command Encryption Module	Mitsubishi Space Software Co., Ltd.	Firmware Version: 2.0
1688	03/09/2012	Momentus® FDE Attached Storage Drives FIPS 140 Module	Seagate Technology LLC	Hardware Version: ST9500326AS; Firmware Version: 566
1689	03/09/2012	Cisco Unified IP Phone 7906G, 7911G, 7931G, 7941G, 7942G, 7945G, 7961G, 7961GE, 7962G, 7965G, 7970G, 7971G, 7971GE and 7975G	Cisco Systems, Inc.	Hardware Versions: (CP-7906G: V01-V09), (CP-7911G: V01-V09), (CP-7931G: V01-V05), (CP-7941G: V01-V02), (CP-7942G: V01-V10), (CP-7945G: V01-V11), (CP-7961G: V01-V02), (CP-7961GE: V01), (CP-7962G: V01-V11), (CP-7965G: V01-V11), (CP-7970G: V01-V02), (CP-7971G/7971GE: V01-V03) and (CP-7975G: V01-V12); Firmware Version: 9.2(1)SR2
1690	03/09/2012	Protiva PIV v1.55 on TOP DL v2	Gemalto	Hardware Version: A1023378; Firmware Version: Build#11 - M1005011+ Softmask V03, Applet Version: Protiva PIV v1.55
1691	03/09/2012			

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1692	03/12/2012	IBM® z/OS® Version 1 Release 13 System SSL Cryptographic Module	IBM® Corporation	Hardware Version: FC3863 w/System Driver Level 86E, and optional CEX3A and CEX3C [CEX3A and CEX3C are separately configured versions of 4765-001 (P/N 45D6048)]; Software Version: System SSL level HCPT3D0/JCPT3D1 w/ APAR OA36775, RACF level HRF7780 and ICSF level HCR7780 w/ APAR OA36882; Firmware Version: 4765-001 (e1ced7a0)
1693	03/28/2012	Luna® PCI-e Cryptographic Module	SafeNet, Inc.	Hardware Versions: VBD-05-0100 and VBD-05-0101; Firmware Version: 6.2.1
1694	03/30/2012	Luna® PCI-e Cryptographic Module	SafeNet, Inc.	Hardware Version: VBD-05-0100 and VBD-05-0101; Firmware Version: 6.2.1
1696	03/28/2012	HIBUN Cryptographic Module for User-Mode	Hitachi Solutions, Ltd.	Software Version: 1.0 Rev. 2
1697	03/28/2012	HIBUN Cryptographic Module for Kernel-Mode	Hitachi Solutions, Ltd.	Software Version: 1.0 Rev. 2
1698	03/28/2012	HIBUN Cryptographic Module for Pre-boot	Hitachi Solutions, Ltd.	Software Version: 1.0 Rev. 2
1699	03/28/2012	McAfee EMM Cryptographic Module	McAfee, Inc.	Software Version: 1.0
1700	03/28/2012	Cisco 881W and Cisco 881GW Integrated Services Routers (ISRs)	Cisco Systems, Inc.	Hardware Versions: 881W and 881GW with [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0]; Firmware Version: Router Firmware Version: IOS 15.1(3)T2 and AP Firmware Version: 12.4(25d)JA1
1701	03/30/2012	Apple FIPS Cryptographic Module	Apple Inc.	Software Version: 1.1